METHOD AND SYSTEM FOR PROVIDING ACCESS TO ELEMENTS ON A CONTROL AREA NETWORK

RELATED APPLICATIONS

This application is related to U.S. Provisional Patent Application Serial No. _____ (006287.0103), entitled "SYSTEM AND METHOD FOR INTERACTING WITH THE INTERNET AS A CONTROL NETWORK DEVICE" and Filed April 29, 1999.

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to the field of network communication, and more particularly to a system and method for interacting with the internet as a control network device.

BACKGROUND OF THE INVENTION

In a fully automated environment, appliances that change the various parameters of the environment can be inked to a control area network (CAN) and a computer-based controller. The appliances may include heating, ventilation and air conditioning (HVAC) systems, lighting systems, audio-visual systems, telecommunications systems, security systems, surveillance systems, and fire protection systems, for example. One or more easy-to-use user interface, such as a touch panel, may be electronically linked to the control area network to accept user input and display current system status. One problem arises when an application operating in one protocol wants to communicate with an appliance or device which operates in a second protocol. A second problem arises when an application or user attempts to access an off-limit area. AMX Corporation of Dallas, Texas designs and manufactures such networked appliance control systems.

SUMMARY OF THE INVENTION

The present invention provides a method and system for providing access to elements on a control area network that substantially eliminate or reduce the disadvantages and problems associated with network access systems.

In one aspect of the invention, Internet applications such as web browsers and applications executing on web servers of information content providers can connect to devices on the control area network which use a different protocol. The Internet applications are capable of sending commands to and receiving commands from devices on the control area network.

In another aspect of the invention, Internet applications such as web browsers and applications executing on web servers of information content providers are blocked from access certain devices on the control area network or even a control area network.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, wherein like reference numerals represent like parts, in which:

FIGURE 1 is a simplified top-level block diagram of a system and method of Internet control system which couple one or more control systems to the Internet constructed according to the teachings of the present invention;

FIGURE 2 is a more detailed block diagram of a system and method of coupling one or more control system to the Internet constructed according to an embodiment of the present invention; and,

FIGURE 3 is a diagram illustrating a system for cloaking IP addresses.

DETAILED DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a simplified top-level block diagram of a system and method 10 of Internet control system which couple one or more control systems to the Internet constructed according to the teachings of the present invention. The implications of employing system and method 10 of the present invention are the ability to communicate with, control, and be controlled by one or more Internet nodes or Internet applications that act as one or more devices in a control system connected by a control area network (CAN). These Internet applications may include web browsers, web server applications of information content providers, and email applications. In other words, the geographical and communication protocol boundaries are transparent between a local control area network and the Internet, so that the Internet, web information content providers and web browser applications become devices in the control system. By definition, a device in the control system can send control commands to and/or receive control messages from a master controller on the control area network. Hereinafter, the word Internet may be also used to refer to an Intranet or the World Wide Web and vice versa.

System 10 includes a control network portal 12 coupled between the Internet 22 and one or more control area networks 30 and 31. Control area networks 30 and 31 are local area networks operating under transport protocols such as Ethernet, and AXLink and PhastLink of AMX Corporation (Dallas, Texas) that interconnect a variety of devices, appliances and/or equipment. The underlying network connectivity 34 may be wired, wireless, power line carriers, or any suitable transmission medium. Coupled to control area networks 30

and 31 are a plurality of devices, appliances and/or equipment, including control area network user interfaces (CAN UI/F) 35, master controllers 36, and Internet appliances 37-39. Some devices may be coupled to control area networks 30 and 31 via additional intermediate communications devices, such as an RS 232 controller (not shown).

Control area network user interface device 35 is any device that is capable of receiving user input and displaying or indicating control network status. For example, a touch panel, a computer terminal with a monitor, keyboard and pointing device, and any device with similar functionalities may serve as control area network user interface 35. As described in detail below, with the use of control area network portal 12 of the present invention, Internet applications are also capable of functioning as control area network user interface devices without the use of custom and dedicated applications on the user's end.

Master controller 36 is generally a CPU-based controller that controls the communications among user interface 35 and Internet appliances 37-39. It is operable to receive user inputs received by user interface devices, such as commands, and instruct the appropriate Internet appliance to act according to the command. Master controller 36 may also poll each device in control area network 30 periodically to monitor its status. The system status and/or the status of each device may be sent to control area network user interface devices for display.

Internet appliances 37-39 are devices that can receive commands from master controller 36 and operate or act according to the command. Internet appliances 37-39 may include equipment that affect or monitor the various parameters of the premises. For example, Internet

appliances 37-39 may include heating and air conditioning, lighting, video equipment, audio equipment, sprinklers, security cameras, infrared sensors, smoke detectors, etc. in a residential or commercial control area network. Household appliances, such as a hot tub, fireplace, microwave oven, coffee maker, etc. may also be Internet appliances coupled to the network. Internet appliances 37-39 may also be capable of providing a current status of its operational state to master controller 36, such as on/off, temperature settings, current ambient temperature, light intensity settings, volume settings, threshold settings, and predetermined alphanumeric strings reflective of operational states.

Master controller 36 is also operable to receive user input from nodes of the Internet 22 via control network portal 12. Connected to Internet 22 are content providers 25 and 26, which may also function as control area network user interface devices. Content providers 25 and 26 are typically web servers that generate and provide static and/or dynamic information and content in the form of web pages. Content provider applications executing on the web server are able to mine data stored in databases (not shown). The web pages are typically developed with hypertext markup language (HTML), and various other scripting languages and programming environments such as Microsoft Active Server Pages (ASP), Common Gateway Interface (CGI), Internet Server Application Programming Interface (ISAPI), JAVA, ActiveX, Cold Fusion, etc. that make the web pages more dynamic and interactive.

Also connected to the Internet 22 are web browsers 23 and 24 that may also serve as control area network user interfaces. Web browsers 23 and 24 are application programs that can be used to request web pages from

content providers 25 and 25 and decode the web pages. Web browser applications include NETSCAPE NAVIGATOR and MICROSOFT INTERNET EXPLORER, for example. Typically, a user executes a web browser application on her personal computer and accesses the World Wide Web via a dial-up connection to an Internet service provider. The Internet or World Wide Web may also be accessed via other means such as cable modems and digital subscriber lines (DSL). The user makes a request for a particular web page or particular web site by entering or specifying a uniform resource locator (URL). The URL is associated with an Internet protocol (IP) address of the specified web site. Every computer connected to the World Wide Web and Internet has a unique IP address. This address is used to route message packets to specific computers and users. Internet protocol or IP is the message transport and communications protocol of the Internet and World Wide Web.

When the web browser requests a certain URL, a connection is first established with a web server of a content provider that is addressed by the URL. A hypertext transport protocol (HTTP) request is then issued to the web server to download an HTML file. The web server receives the request and sends a web page file to the web browser, which decodes the file to display information in specified format on the screen. Web pages with dynamic content provided by gateway interfaces such as CGI and ISAPI are executable applications that are ran by the web server upon user request. The executing gateway application is able to read parameter information associated with the request and generate an output in the form of an HTML file in response to the parameter values. Another way to add dynamic and interactive content to web pages uses ASP. ASP scripts are server-side executable

scripts that are directly incorporated in the HTML web pages. Upon request for the page, the web server executes the ASP script in response to input parameter values and generates the web page with dynamic content.

Using control network portal 12, users may access control area networks 30 and 31 via web browsers 23 and 24 accessing web pages provided by control network portal 12 or value-added web pages provided by content providers 25 and 26. For example, a user who has a control area network deployed in his luxury residence to control various aspects of the home environment may use a web browser application to remotely monitor his home. He may change the temperature setting to decrease energy use, for example, because he will be leaving on a business trip straight from work. He may also use the surveillance cameras to visually ensure security has not been breached. He may even be able to remotely program his VCR to record certain favorite programs that will be broadcast while he is away.

An example of value-added web pages provided by content providers is the provision of an interactive version of the television programming web page, www.tvguide.com. A user may request this web page, determine available program choices, and click on a certain program. Options may be provided to enable the user to turn on the television and tune to a particular channel scheduled to broadcast the selected program or to program the VCR to record the selected program.

Another example of value-added web pages provided by content providers is the provision of a secured web page that an electric company may access to slightly raise the temperature settings of the air conditioning systems of its participating customers in anticipation of high demand brown out conditions. Yet another example is a

web page that a security company may use to access, monitor and control the security, surveillance and fire protection systems of its customers.

FIGURE 2 is a more detailed block diagram of a system and method 10 of coupling one or more control system to the Internet constructed according to an embodiment of the present invention. Control area network portal 12 may include a web server 13 coupled to the Internet 22. Web server 13 is also coupled to an Internet appliance (IA) server 14, which may also be coupled to a control network server 40. Control network server 40 is coupled to control area network 30 that links several appliances and systems, such as fire protection systems 50, heating, ventilation and air conditioning (HVAC) systems 51, lighting systems 52, audio and visual systems 53, and security systems 54. Control area network 30 is also coupled to user interface devices 55 and master controller 36.

It may be noted that control network portal 12 may be implemented by a single stand-alone system that has sufficient memory and processing power or several separate systems with distinct functions as shown in FIGURE 2. Web server 13 is operable to receive requests of web pages from web browser 23 and to respond by generating and providing the requested web pages. The information content of the web pages may be dynamically obtained by communicating with IA server 14, which is operable to communicate with master controller 36 via control network server 40 to obtain status and other information. Control network server 40 is used only if there is protocol conversion or other control issues needed to operate the control area network. It may be thought of, logically, that IA server 14 is directly coupled to the network and functions as a device on the

network. Commands entered at a web browser are sent to web server 13, which relays the commands to master controller 36 via IA server 14 and control network server 40. Master controller 36 then instructs appropriate appliances and/or systems in the control network to act according to the received command.

FIGURE 3 is a diagram illustrating a system for cloaking IP addresses. Illustrated are content providers 25 and web browsers 23 connected to the internet 22. Also connected to the internet 22 is control area network 31 having a plurality of internet appliances 64, 66, and 68 attached. Also connected is master controller 36 as well as touchpanel 62 and an AXB-NET 60.

In operation, an application operable to use the internet protocol (IP) needs to address or access a device on control area network 31. The device can be an internet appliance 64, 66, 68. The device, however, does not conform to the internet protocol. The application initiates connection with the non-IP device using an IP address and Port number. The connection is routed through the internet to the control master 36. Control master 36 receives the IP connection request. It then can spawn (or access an existing) virtual IP/CAN device and spawn a connection object. The connection object completes the connection by mapping the IP address and port used by the IP application with the actual connection address used by the device. Virtual device 70 acts as a protocol translator, translating IP messages into a format useable by the non-IP device. In this fashion, the IP application acts as if it is communicating with an IP device. Communication can occur in both direction. Even though IP and non-IP addressing was discussed other protocols can be used.

In another embodiment, an application such as web browser 23 may attempt to access a device such as an internet appliance, touchpad 62 or even an entire control area network 31. For security or other reasons access to the internet appliance, touchpad 62 or control area network 31 is forbidden. In this case, when a request to access the device is received by the control master 36, the connection object 72 will indicate that connection to that device is forbidden and a message will be sent back the web browser or other internet application.

Though the invention has been described with respect to a specific embodiment thereof, many variations and modifications may be apparent to those skilled in the art. It is therefore the intention that the appended claims be interpreted as broadly as possible to include all such variations and modifications.

WHAT IS CLAIMED IS:

1. A control system, comprising:

at least one IP application;

a control area network interconnecting the at least one IP application and having at least one non-IP device connected;

a network located between the control area network and the at least one IP application; and

a master controller coupled to the network and operable to spawn a connection object operable to allow communication between the at least one IP application and the at least one non-IP device.

2. The control system, as set forth in claim 1, further comprising at least one user interface coupled to the network and in communication with the master controller.

3. The control system, as set forth in claim 2, wherein the at least one user interface each comprises:

a display; and

a user input device operable to receive a user input.

4. The control system, as set forth in claim 2, wherein the at least one user interface each comprises:

a control system status indicator; and

a user input device operable to receive a user input.

5. The control system, as set forth in claim 1, wherein the control network portal comprises a web server

coupled to the Internet and operable to receive requests from the Internet and to service the received requests.

6. The control system, as set forth in claim 1, wherein the control network portal comprises an Internet appliance server coupled to the Internet and operable to pass command messages therebetween.

7. The control system, as set forth in claim 6, wherein the Internet appliance server comprises a software device emulator operable to spawn a software logical device for the Internet, thereby commands from the master controller destined for the Internet are delivered to the software logical device.

8. The control system, as set forth in claim 6, wherein the Internet appliance server comprises:

at least one software logical device representative of the Internet; and

at least one software logical device representative of a device in the network.

9. The control system, as set forth in claim 1, further comprising a virtual device protocal translator operable to translate the IP messages from the IP appliance to a format understood by the non-IP address.

10. The control system, as set forth in claim 1, wherein the control master spawns the IP connection object but mapping fails because access to the device is denied.

11. A method for communicating over a network comprising:

providing at least one IP application;

providing a control area network interconnecting the at least one IP application and having at least one non-IP device connected;

providing a network located between the control area network and the at least one IP application; and

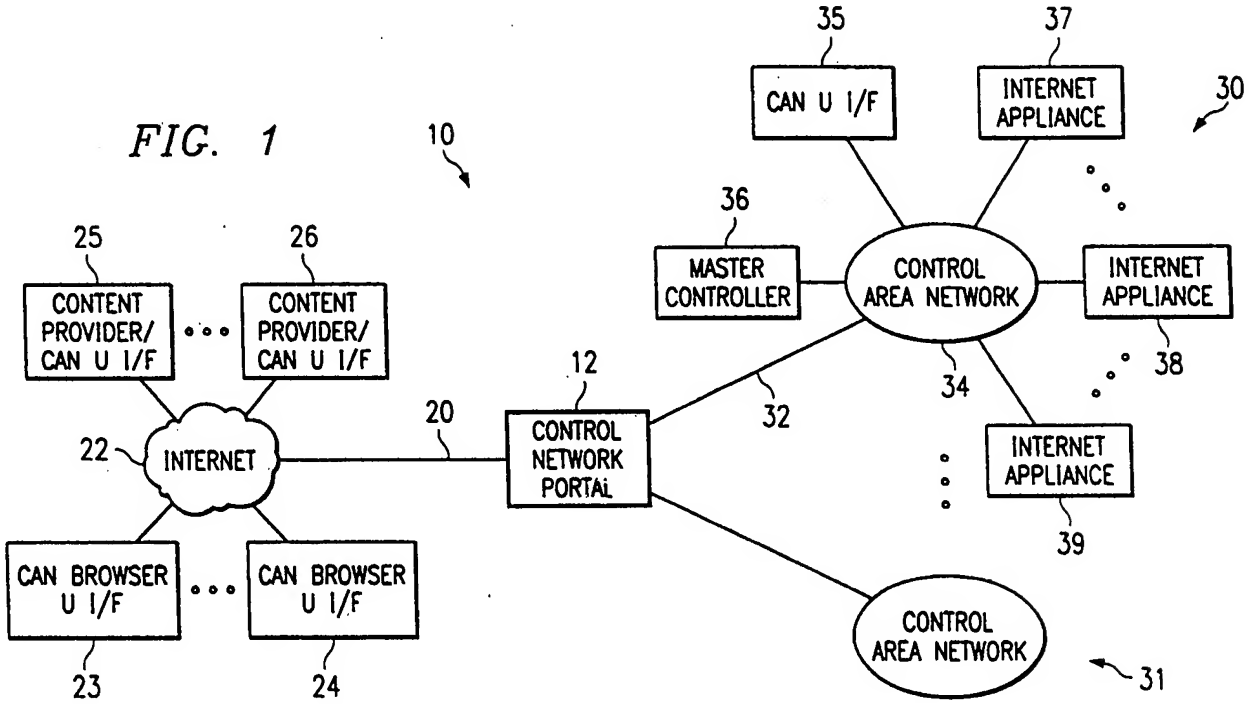
providing a master controller coupled to the network and operable to spawn a connection object operable to allow communication between the at least one IP application and the at least one non-IP device.

METHOD AND SYSTEM FOR PROVIDING ACCESS TO ELEMENTS ON A CONTROL AREA NETWORK

ABSTRACT OF THE DISCLOSURE

A method and system for providing access to a control area network is provided. An IP-appliance communicates to a non-IP device through the Internet. This is because the control master spawns IP connection object that maps the IP address with the non-IP address to allow a connection to occur that is transparent to the IP application.

FIG. 1


10
12
20
22
25
26
CONTENT PROVIDER/ CAN U I/F
CONTENT PROVIDER/ CAN U I/F
INTERNET
CONTROL NETWORK PORTAL
CAN BROWSER U I/F
CAN BROWSER U I/F
23
24
30
31
32
34
35
CAN U I/F
36
MASTER CONTROLLER
37
INTERNET APPLIANCE
CONTROL AREA NETWORK
INTERNET APPLIANCE
38
INTERNET APPLIANCE
39
CONTROL AREA NETWORK

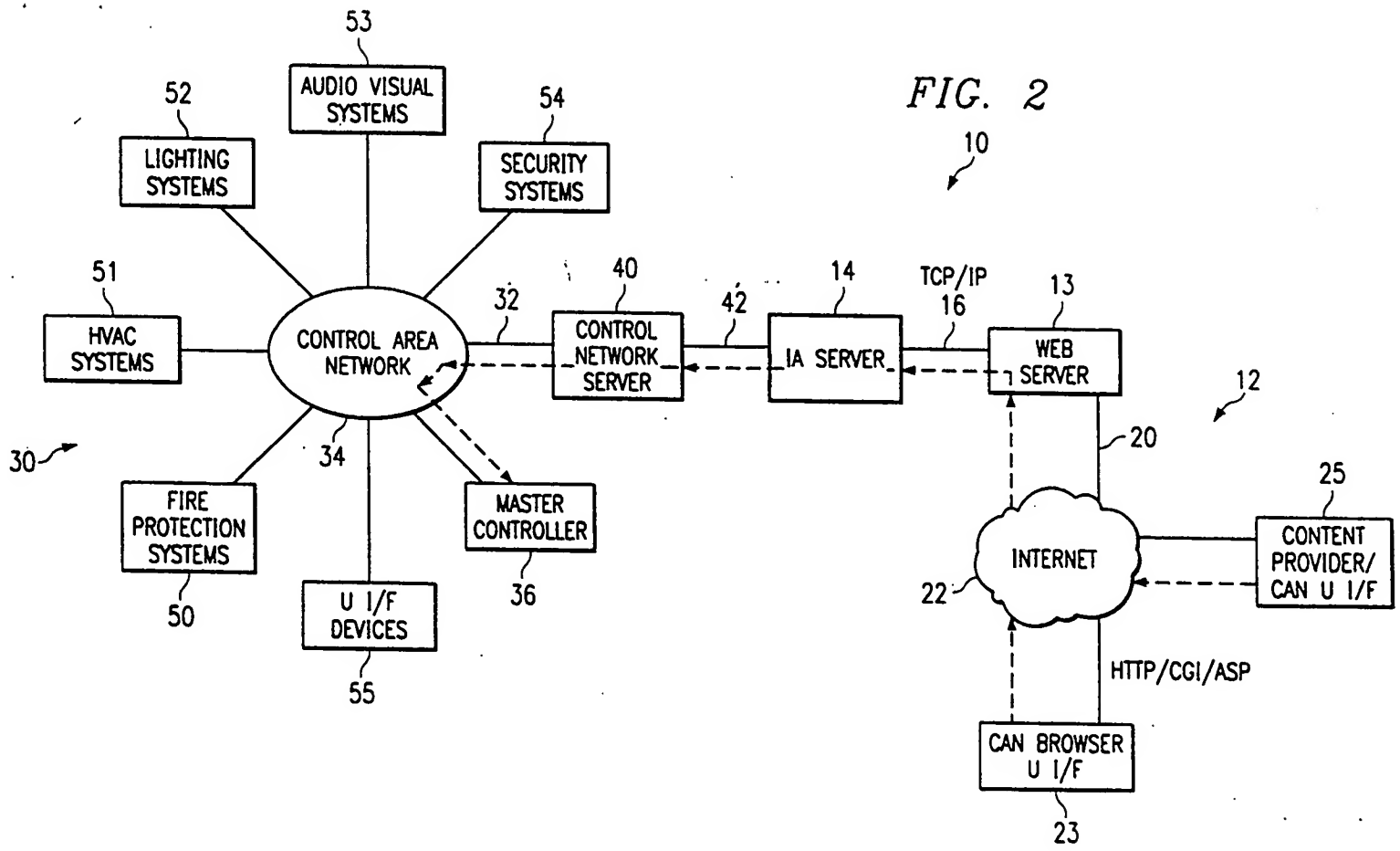


FIG. 2

2 of 3

IP Device Cloaking in Control Systems

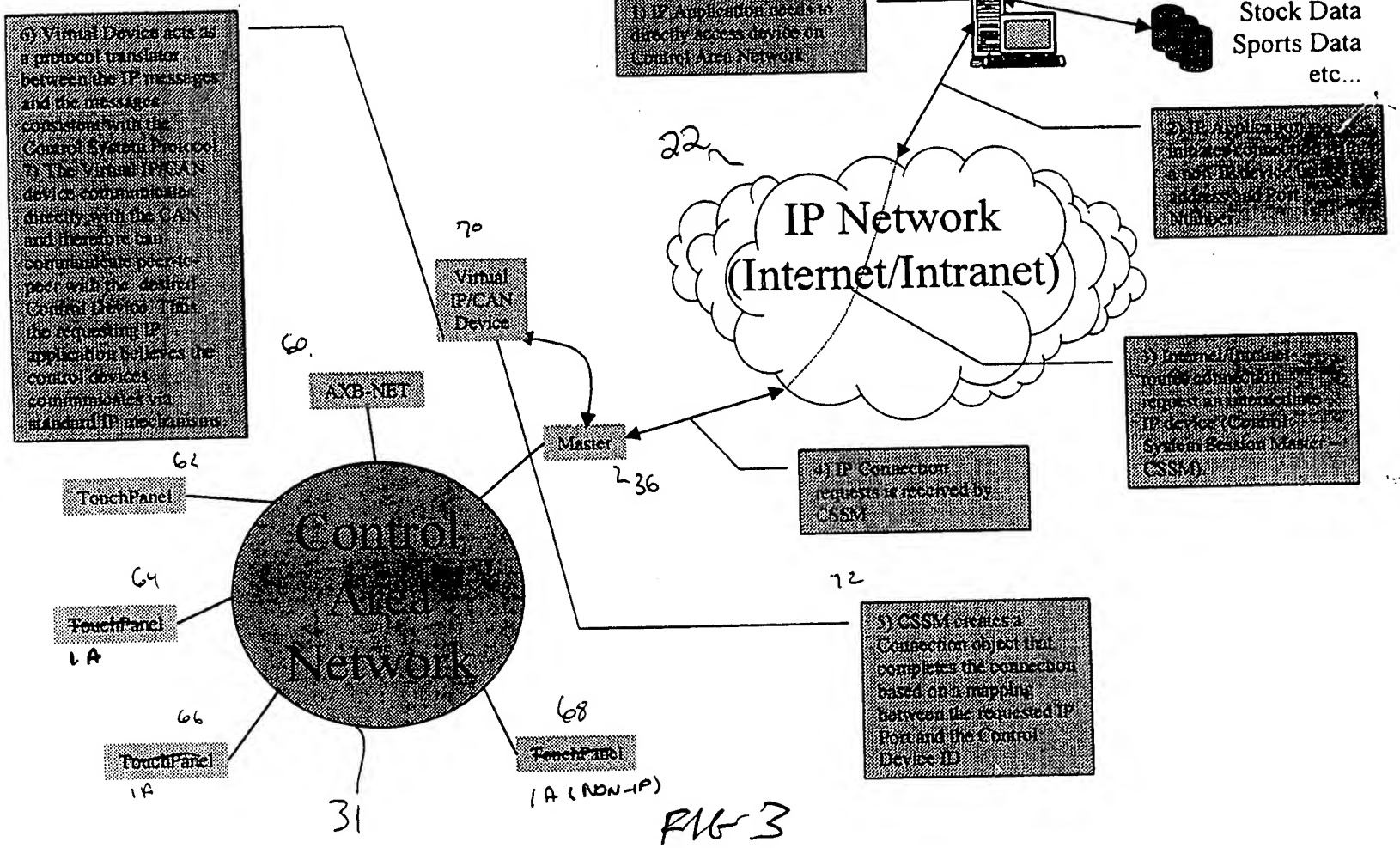


FIG 3